UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,078	11/18/2003	Oleksiy Pikalo	BBNT-P02-097	4787

28120 7590 02/02/2009

ROPES & GRAY LLP
PATENT DOCKETING 39/41
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
02/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/716,078	PIKALO ET AL.	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-62* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8,9,11-21,23,24,26-36,39,41-50,52-58 and 60-62* is/are rejected.

7)☒ Claim(s) *6,7,10,22,25,37,38,40,51 and 59* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This non-final action is in response to the Request for Continued Examination filing of 11/17/2008. Claims 1-62 are pending and have been considered as follows.

Examiner Note

The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claim 62 by using "means-plus-function" language. The Examiner notes that the claims appear to pass all of the three-prong test used to determine invocation of paragraph 6. Therefore, 35 U.S.C. 112 6th paragraph has been invoked when considering these claims below.

> *A claim limitation will be presumed to invoke 35 U.S.C. 112, sixth paragraph, if it meets the following 3-prong analysis:*
> *(A) the claim limitations must use the phrase "means for " or "step for; "*
> *(B) the "means for " or "step for " must be modified by functional language; and*
> *(C) the phrase "means for " or "step for " must not be modified by sufficient structure, material, or acts for achieving the specified function.*

Allowable Subject Matter

1. Claims 6, 7, 10, 22, 25, 37, 38, 40, 51, & 59 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

- The examiner notes that these limitations and particularly in combination with the aspects found in their parent claims which clarify precisely how the applicants' invention achieves the controlling/adjusting of "path length" which appears if brought into independent form would better distinguish the applicants' invention from the prior art of record;
- The examiner also notes that the current claim language does not clearly claim what appears to be correction for phase error as suggested by the applicants' dependent limitations and Specification, perhaps better clarity with respect to this limitation would also better distinguish the applicants' invention from the prior art of record;

Claim Objections

2. Claim 15 is objected to because of the following informalities:

- Claim 15 line 3 appears to be missing the term "training" before "...symbols...";

Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 11-13, 26, 27, & 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang (US-20030002670-A1).

Claim 1:

Wang discloses a method of controlling path length in a quantum cryptographic key distribution (QKD) system comprising,

- "receiving a signal identifying a plurality of (symbols as training symbols) over a QKD path" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];
- "receiving the plurality of (training symbols) transmitted from a QKD transmitter over the QKD path via quantum cryptographic mechanisms" (i.e. "a successful detection of a first and second idler beam (i1, i2) photon by the idler beam detector 220") [page 4 para 33];
- "controlling a length of the QKD path based on the received plurality of (training symbols)" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

Claim 11:

Wang discloses a system configured to automatically initialize a length of a quantum cryptographic key distribution (QKD) path in a QKD system comprising,

- "a QKD receiver configured to determine whether (training symbols) are to be received and to receive training symbols from a QKD transmitter over the QKD path" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];
- "a phase shifting element disposed on the QKD path" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

- "processing logic configured to automatically initialize the length of the QKD path, using the phase shifting element, based on the received (training symbols)" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

Claim 12:

Wang discloses a computer-readable memory device containing instructions configured to control at least one processor to perform a method of controlling path length in a quantum cryptographic key distribution (QKD) system comprising,

- "receiving a signal identifying a plurality of (symbols) as (training symbols) over a QKD path" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];

- "receiving the plurality of (training symbols) transmitted from a QKD transmitter over the QKD path via quantum cryptographic mechanisms" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];
- "controlling a length of the QKD path based on the plurality of received (training symbols)" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

Claim 13:

Wang discloses a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer comprising,

- "employing a phase shifting element in the second interferometer" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];
- "automatically adjusting the phase shifting element to control the path length based on (training symbols) transmitted over the path via quantum cryptographic mechanisms" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];
- "where the (training symbols) are distinguished from other types of (symbols) transmitted over the path" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

Claim 26:

Wang discloses a system configured to automatically control a path length in a quantum cryptographic key distribution (QKD) system comprising,

- "a QKD path including a first interferometer and a second interferometer" (i.e. "A first light modulator…second light modulator") [page 3 para 26];
- "a phase shifting element disposed in at least one of the first and second interferometers" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];
- "processing logic configured to automatically adjust the phase shifting element to control a length of the path based on (training symbols) transmitted over the QKD path via quantum cryptographic mechanisms" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];
- "where the (training symbols) are distinguished from other types of (symbols) transmitted over the path" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon... phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

Claim 27:

Wang discloses a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system comprising,

- "employing a feedback system in the QKD system" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];
- "where the QKD system comprises a first interferometer and a second interferometer" (i.e. "A first light modulator...second light modulator") [page 3 para 26];
- "receiving (training symbols) transmitted over the path from the first interferometer to the second interferometer via quantum cryptographic mechanisms" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];

- "where the (training symbols) are distinguished from other types of (symbols) transmitted over the path" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];
- "automatically controlling the path length, using the feedback system, based on the (training symbols) transmitted over the path from the first interferometer to the second interferometer" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

Claim 41:

Wang discloses a quantum cryptographic key distribution (QKD) endpoint comprising,

- "a QKD receiver configured to receive (symbols) transmitted over a QKD path via quantum cryptographic mechanisms" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication") [page 4 para 33];
- "distinguishing (training symbols) from data (symbols) in the received (symbols)" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];
- "a feedback system configured to control a length of the QKD path based on the received (training symbols)" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols," in the invention as disclosed by Wang for the purposes of providing a means for feedback.

5. Claims 2-5, 8, 9, 52-58, & 60-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang (US-20030002670-A1) in view of Page (US-5157461-A).

Claim 2:

Wang discloses a method of controlling path length in a quantum cryptographic key distribution (QKD) system, and in Claim 1 above, but Wang does not explicitly disclose,

- "estimating a phase error associated with transmission of the training symbols over the QKD path," although Page does suggest estimation error computations, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with transmission of the training symbols over the QKD path," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 3:

Wang and Page disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, and in Claim 2 above, but Wang does not explicitly disclose,

- "determining probabilities of detection events associated with the received training symbols," although Page does suggest detection and response to signal intensity, as recited below;

however, Page does disclose,

- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining probabilities of detection events associated with the received training symbols," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 4:

Wang and Page disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, and in Claim 3 above, but Wang does not explicitly disclose,

- "estimating the phase error based on the determined probabilities," although Page does suggest estimation of error based on statistical effects, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating the phase error based on the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 5:

Wang and Page disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, and in Claim 2 above, but Wang does not explicitly disclose,

- "controlling the length of the QKD path based on the estimated phase error," although Page does suggest utilizing a Kalman filter for providing better estimate to counter error due to noise, as recited below;

however, Page does disclose,

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "controlling the length of the QKD path based on the estimated phase error," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 8:

Wang and Page disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, and in Claim 2 above, but Wang does not explicitly disclose,

- "employing at least one Kalman filter to estimate the phase error," although Page does suggest utilizing a Kalman filter for providing better estimate to counter error due to noise, as recited below;

however, Page does disclose,

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "employing at least one Kalman filter to estimate the phase error," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 9:

Wang and Page disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, and in Claim 4 above, but Wang does not explicitly disclose,

- "performing a robust least squares estimation of the phase error using the determined probabilities," although Page does suggest utilizing a Kalman filter for providing better estimate to counter error due to noise, as recited below;

however, Page does disclose,

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "performing a robust least squares estimation of the phase error using the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 52:

Wang discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system comprising,

- "receiving one or more (symbols) that indicate that a subsequent sequence of (symbols) comprises (training symbols)" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication… a successful detection of a first and second idler beam (i1, i2) photon by the idler beam detector 220") [page 4 para 33];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;
- "determining probabilities associated with a plurality of detection events," although Page does suggest error computation and statistical effects of residual noise, as recited below;
- "the plurality of detection events being associated with the training symbols received over the path in the QKD system via quantum cryptographic mechanisms," although Page does suggest a detection circuit responsive to a signal, as recited below;
- "controlling the length of the path based on the determined probabilities," although Page does suggest utilizing a Kalman filter to provide optimal estimation techniques for a signal, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

whereas, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];
- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols" and "determining probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with the training symbols received over the path in the QKD system via quantum cryptographic mechanisms" and "controlling the length of the path based on the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 53:

Wang and Page disclose a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 52 above, but Wang does not explicitly disclose,

- "the probabilities comprise conditional probabilities," although Page does suggest error computation and statistical effects of residual noise, as recited below;

however, Page does disclose,

- "the statistical effects of the previously-described residual noise" [column 18 lines 23-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the probabilities comprise conditional probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 54:

Wang and Page disclose a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 52 above, but Wang does not explicitly disclose,

- "estimating a phase error based on the determined probabilities," although Page does suggest error computation and statistical effects of residual noise, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error based on the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 55:

Wang and Page disclose a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, but Wang does not explicitly disclose,

- "controlling the path length of the QKD path further based on the estimated phase error," although Page does suggest error computation and statistical effects of residual noise, as recited below;

however, Page does disclose,

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "controlling the path length of the QKD path further based on the estimated phase error," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 56:

Wang and Page disclose a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, but Wang does not explicitly disclose,

- "performing a least squares estimation of the phase error using the determined probabilities," although Page does suggest error computation and statistical effects of residual noise, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "performing a least squares estimation of the phase error using the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 57:

Wang and Page disclose a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, but Wang does not explicitly disclose,

- "employing at least one Kalman filter to estimate the phase error," although Page does suggest error computation and statistical effects of residual noise, as recited below;

however, Page does disclose,

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "employing at least one Kalman filter to estimate the phase error," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 58:

Wang and Page disclose a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, but Wang does not explicitly disclose,

- "performing a robust least squares estimation of the phase error using the determined probabilities," although Page does suggest error computation and statistical effects of residual noise, as recited below;

however, Page does disclose,

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "performing a robust least squares estimation of the phase error using the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claim 60:

Wang discloses a quantum cryptographic key distribution (QKD) endpoint comprising,

- "a QKD receiver configured to receive a sequence of (symbols) transmitted over a QKD path via quantum cryptographic mechanisms" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication… a successful detection of a first and second idler beam (i1, i2) photon by the idler beam detector 220") [page 4 para 33];
- "a phase shifting element disposed on the QKD path" (i.e. "When there is a discrepancy, the necessary phase change is adjusted to ensure that the encryption key string transmission occurs at a higher successful rate") [page 4 para 34];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;

- "processing logic configured to: determine, based on determining that the sequence of symbols corresponds to a sequence of training symbols, conditional probabilities associated with a plurality of detection events," although Page does suggest error computation and statistical effects of residual noise, as recited below;
- "the plurality of detection events being associated with the sequence of symbols," although Page does suggest a detection circuit responsive to a signal, as recited below;
- "processing logic configured to: adjust the phase shifting element to control a length of the QKD path based on the determined conditional probabilities," although Page does suggest utilizing a Kalman filter to provide optimal estimation techniques for a signal, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

whereas, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols" and "processing logic configured to: determine, based on determining that the sequence of symbols corresponds to a sequence of training symbols, conditional probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with the sequence of symbols" and "processing logic configured to: adjust the phase shifting element to control a length of the QKD path based on the determined conditional probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claims 61 & 62:

Wang discloses a computer-readable memory device containing instructions configured to control at least one processor to perform a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system and a system configured to control a length of a path in a quantum cryptographic key distribution (QKD) system comprising,

- "means for receiving one or more symbols that indicate that a subsequent sequence of symbols comprises training symbols" (i.e. "First, the sender 202 uses the detection of the first and second idler beam (i1, i2) photons by the idler beam single-photon detector 220 as a condition for a successful communication… a successful detection of a first and second idler beam (i1, i2) photon by the idler beam detector 220") [page 4 para 33];

but, Wang does not explicitly disclose,

- "symbols" and "training symbols," although Wang does suggest utilizing specialized photons for feedback and adjusting phase change, as recited below;
- "determining probabilities associated with a plurality of detection events," although Page does suggest error computation and statistical effects of residual noise, as recited below;
- "the plurality of detection events being associated with the training symbols received over the path in the QKD system via quantum cryptographic mechanisms," although Page does suggest a detection circuit responsive to a signal, as recited below;
- "controlling the length of the path based on the determined probabilities," although Page does suggest utilizing a Kalman filter to provide optimal estimation techniques for a signal, as recited below;

however, Wang does disclose,

- "a first or second signal beam (s1, s2) photon… phase change is adjusted" [page 4 para 33 & 34];

whereas, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];

- "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art" [column 16 lines 51-54];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "symbols" and "training symbols" and "determining probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with the training symbols received over the path in the QKD system via quantum cryptographic mechanisms" and "controlling the length of the path based on the determined probabilities," in the invention as disclosed by Wang for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

6. Claims 14-17, 28-32, & 42-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang (US-20030002670-A1) in view of Ahn et al. (US-6160627-A).

Claims 14-17:

Wang discloses a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, but, Wang does not explicitly disclose,

- "the phase shifting element comprises a fiber stretcher," although Ahn et al. does suggest a fiber stretcher, as recited below;
- "adjusting a voltage applied to the fiber stretcher based on the symbols transmitted over the path," although Ahn et al. does suggest a fiber stretcher, as recited below;

- "the phase shifting element comprises a phase modulator," although Ahn et al. does suggest a fiber stretcher connected with two light paths of an interferometer, as recited below;
- "adjusting a voltage applied to the phase modulator based on the training symbols transmitted over the path," although Ahn et al. does suggest an optical fiber phase modulator, as recited below;

however, Ahn et al. does disclose,

- "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the phase shifting element comprises a fiber stretcher" and "adjusting a voltage applied to the fiber stretcher based on the symbols transmitted over the path" and "the phase shifting element comprises a phase modulator" and "adjusting a voltage applied to the phase modulator based on the training symbols transmitted over the path," in the invention as disclosed by Wang for the purposes of providing a means for phase modulation.

Claims 28-32:

Wang discloses a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, but, Wang does not explicitly disclose,

- "the feedback system comprises a phase shifting element," although Ahn et al. does suggest a phase modulator, as recited below;

- "the phase shifting element comprises a fiber stretcher," although Ahn et al. does suggest a fiber stretcher, as recited below;
- "adjusting a voltage applied to the fiber stretcher based on the training symbols transmitted over the path," although Ahn et al. does suggest a fiber stretcher, as recited below;
- "the phase shifting element comprises a phase modulator," although Ahn et al. does suggest a fiber stretcher connected with two light paths of an interferometer, as recited below;
- "adjusting a voltage applied to the phase modulator based on the training symbols transmitted over the path," although Ahn et al. does suggest an optical fiber phase modulator, as recited below;

however, Ahn et al. does disclose,

- "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the feedback system comprises a phase shifting element" and "the phase shifting element comprises a fiber stretcher" and "adjusting a voltage applied to the fiber stretcher based on the training symbols transmitted over the path" and "the phase shifting element comprises a phase modulator" and "adjusting a voltage applied to the phase modulator based on the training symbols transmitted over the path," in the invention as disclosed by Wang for the purposes of providing a means for phase modulation.

Claims 42-44:

Wang discloses a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, but, Wang does not explicitly disclose,

- "the feedback system comprises a phase shifting element," although Ahn et al. does suggest a phase modulator, as recited below;
- "the phase shifting element comprises a fiber stretcher," although Ahn et al. does suggest a fiber stretcher, as recited below;
- "the phase shifting element comprises a phase modulator," although Ahn et al. does suggest a fiber stretcher connected with two light paths of an interferometer, as recited below;

however, Ahn et al. does disclose,

- "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the feedback system comprises a phase shifting element" and "the phase shifting element comprises a fiber stretcher" and "the phase shifting element comprises a phase modulator," in the invention as disclosed by Wang for the purposes of providing a means for phase modulation.

7. Claims 18-21, 23, 24, 33-36, 39, & 45-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wang (US-20030002670-A1) in view of Ahn et al. (US-6160627-A) and in view of in view of Page (US-5157461-A).

Claims 18-21, 23, & 24:

Wang and Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, but, their combination do not explicitly disclose,

- "estimating a phase error associated with symbols transmitted over the path," although Page does suggest estimation error computations, as recited below;
- "determining probabilities of detection events associated with the symbols transmitted over the path," although Page does suggest estimation error computations, as recited below;
- "estimating the phase error based on the determined probabilities," although Page does suggest estimation error computations, as recited below;
- "the phase shifting element is automatically adjusted to control the path length further based on the estimated phase error," although Page does suggest estimation error computations, as recited below;
- "employing at least one Kalman filter to estimate the phase error," although Page does suggest estimation error computations utilizing a Kalman filter, as recited below;
- "performing a robust least squares estimation of the phase error using the determined probabilities," although Page does suggest square estimation error computations, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];
- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with symbols transmitted over the path" and "determining probabilities of detection events associated with the symbols transmitted over the path" and "estimating the phase error based on the determined probabilities" and "the phase shifting element is automatically adjusted to control the path length further based on the estimated phase error" and "employing at least one Kalman filter to estimate the phase error" and "performing a robust least squares estimation of the phase error using the determined probabilities," in the invention as disclosed by Wang and Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claims 33-36 & 39:

Wang and Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, but, their combination do not explicitly disclose,

- "estimating a phase error associated with symbols transmitted over the path," although Page does suggest estimation error computations, as recited below;
- "determining probabilities of detection events associated with the symbols transmitted over the path," although Page does suggest estimation error computations, as recited below;
- "estimating the phase error based on the determined probabilities," although Page does suggest estimation error computations, as recited below;
- "the phase shifting element is automatically adjusted to control the path length further based on the estimated phase error," although Page does suggest estimation error computations, as recited below;
- "performing a robust least squares estimation of the phase error using the determined probabilities," although Page does suggest square estimation error computations, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];
- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with symbols transmitted over the path" and "determining probabilities of detection events associated with the symbols transmitted over the path" and "estimating the phase error based on the determined probabilities" and "the phase shifting element is automatically adjusted to control the path length further based on the estimated phase error" and "performing a robust least squares estimation of the phase error using the determined probabilities," in the invention as disclosed by Wang and Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Claims 45-50:

Wang and Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 13 above, but, their combination do not explicitly disclose,

- "estimate a phase error associated with the symbols transmitted over the QKD path based on the received symbols," although Page does suggest estimation error computations, as recited below;

- "determine probabilities of detection events associated with the symbols transmitted over the QKD path," although Page does suggest estimation error computations, as recited below;
- "estimating the phase error based on the determined probabilities," although Page does suggest square estimation error computations, as recited below;
- "the estimation system comprises a least squares estimator," although Page does suggest estimation error computations, as recited below;
- "the estimation system comprises at least one Kalman filter," although Page does suggest estimation error computations utilizing a Kalman filter, as recited below;
- "estimation system comprises a robust least squares estimator," although Page does suggest square estimation error computations, as recited below;

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];
- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimate a phase error associated with the symbols transmitted over the QKD path based on the received symbols" and "determine probabilities of detection events associated with the symbols transmitted over the QKD path" and "estimating the phase error based on the determined probabilities" and "the estimation system comprises a least squares estimator" and "the estimation system comprises at least one Kalman filter" and "estimation system comprises a robust least squares estimator," in the invention as disclosed by Wang and Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage and in order to provide optical communications error correction.

Response to Arguments

8. Applicant's arguments with respect to claims 1-62 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicants' amendments.

Conclusion

9. The prior art made of record and not directly relied upon is considered pertinent to the applicant's disclosure.

a. Hughes et al. ("Practical quantum key distribution over a 48-km optical fiber network") – quantum key distribution in fiber optic network with adjustment of path length;

b. Dultz et al. (US-6430345-B1) - path length adjustments but not using "symbols/frames" language, suggests details on phase shifting and other noise/interference mitigation/correction techniques;

c. Gisin et al. (US-6438234-B1) - path length adjustments but not using "symbols/frames" language, suggests details on phase shifting and other noise/interference mitigation/correction techniques;

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
01/30/2009

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436